AO 106 (Rev. 04/10) Application for a Search Warrant (USAO CDCA Rev. 01/2013)

ORIGINAL

UNITED STATES DISTRICT COURT

for the

District of Hawaii

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address)
A Silver in Color, "Apple" I-phone, currently located at 91-1300 Enterprise Avenue Kapolei, HI 96707

Case No. Mag. No. 19-00529-KJM

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location):*

See Attachment A

located in the _____ District of Hawaii , there is now concealed *(identify the person or describe the property to be seized)*:

See Attachment B

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☑ evidence of a crime;
- ☑ contraband, fruits of crime, or other items illegally possessed;
- ☑ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
18 U.S.C. § 2113(a)	Bank Robbery

The application is based on these facts:

See attached Affidavit

- ☑ Continued on the attached sheet.
- ☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Applicant's signature

Danielle DeSanctis, Special Agent
Printed name and title

Sworn to before me and signed in my presence.

Date: 6/12/19

Judge's signature

City and state: Honolulu, Hawaii

Hon. Rom Trader, U.S. Magistrate Judge
Printed name and title

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF HAWAII

IN THE MATTER OF THE SEARCH OF A SILVER IN COLOR, "APPLE" IPHONE, CURRENTLY LOCATED AT 91-1300 ENTERPRISE AVENUE, KAPOLEI, HAWAII 96707	MAG NO. 19-00529-KJM AFFIDAVIT IN SUPPORT OF AN APPLICATION UNDER RULE 41 FOR A WARRANT TO SEARCH AND SEIZE

AFFIDAVIT IN SUPPORT OF
AN APPLICATION FOR A SEARCH WARRANT

I, Danielle DeSanctis, a Special Agent ("SA") with the United States Federal Bureau of Investigation ("FBI"), being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a search warrant authorizing the examination of property—an electronic device—which is currently in law enforcement possession, and the extraction from that property of electronically stored information described in Attachment B. Authorization for the requested search and seizure is made based upon probable cause developed during an on-going joint investigation with the FBI Violent Crime Task Force (VCTF), and the Honolulu Police Department (HPD) in the arrest of Ellington R. KEAWE, aka "RAINBOW KEAWE" (KEAWE) for bank robbery, in violation of Title 18, United States Code, § 2113(a). This investigation revealed KEAWE robbed the Bank of Hawaii – Waianae Branch, on May 10, 2019.

2. I have been a Special Agent with the FBI since June 2014. Prior to my current assignment, I was a police officer for the City of Norfolk, Virginia, for six years, reaching the rank of Detective. I am currently assigned to the Hawaii Violent Crime Task Force (VCTF) of the FBI Honolulu Field Office where my duties include, but not limited to, investigating criminal

street gangs and crimes of violence. I am an investigative or law enforcement officer of the United States within the meaning of Section 2510(7) of Title 18, United States Code and empowered by law to conduct investigations of and to make arrests for offenses enumerated in Section 2516 of Title 18, United States Code. Through my training and experience, I have become familiar with the manner in which criminal offenders operate, and the efforts of those involved in such activities.

3. During my tenure as a Police Officer and then with the FBI, I participated in numerous investigations where I have (a) conducted physical and wire surveillance; (b) executed search warrants for electronic devices; (c) reviewed and analyzed numerous taped conversations and records of criminals; (d) debriefed defendants, informants, and witnesses who had personal knowledge regarding the online production and distribution of child pornography; (e) served as a monitor in federal wiretap cases and overheard conversations of drug traffickers to identify subjects and gather evidence; (f) conducted surveillance of individuals engaged in the sexual exploitation of children, drug trafficking, and other violations of federal and state law; (g) arrested offenders for the online production and distribution of child pornography; and (h) arrested offenders for bank robbery.

4. The information contained in this affidavit is based on my personal knowledge and my training, and experiences, information obtained from members of law enforcement personnel, and other witnesses. This affidavit is intended to merely show there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

IDENTIFICATION OF THE DEVICE TO BE EXAMINED

5. The property to be searched is an Apple iPhone 6 Plus, silver in color, hereinafter the "the Subject Device." The Subject Device is currently in the custody of the FBI Honolulu Field Office, located at 91-1300 Enterprise Parkway, Kapolei, Hawaii 96707.

6. The applied-for warrant would authorize the forensic examination of the Device for the purpose of identifying electronically stored data particularly described in Attachment B.

PROBABLE CAUSE

7. On May 10, 2019, at approximately 1506 hours, the Honolulu Police Department ("HPD") patrol units were dispatched to a bank robbery at the Bank of Hawaii ("BOP"), Waianae Branch, located at 86-120 Farrington Highway Waianae, Hawaii 96792. HPD arrived on-scene at approximately 1508 hours, and learned the BOH had been robbed by a lone male subject described below, and later positively identified as KEAWE. The investigation of the bank robbery revealed the following information.

8. On May 10, 2019, S.B., was employed and working as a bank teller at the aforementioned BOH, where she was assigned as "teller 3." At approximately 1453 hours, KEAWE approached S.B.'s teller station dressed in a black, red and white jacket, with a hood pulled down over his eyes, he was also carrying a black in color backpack. KEAWE stated "gimme all your money, I'm robbing you." KEAWE repeated several times "I don't care if they shoot me, give me your money." S.B. made eye contact with BOH manager, F.A., who recognized something was wrong and walked over to S.B.

9. When F.A. arrived at teller station 3, S.B. informed F.A. that KEAWE "wants to rob the bank." KEAWE looked at F.A. and again stated he was robbing the bank and for them to

give him the money or he would "shoot." F.A. did not see a firearm but believed KEAWE possessed one and became fearful for the safety of both her and S.B. F.A. advised S.B. to give KEAWE money from S.B.'s teller drawer.

10. S.B. estimated $2,000, was provided to KEAWE, five (5) of which were "$10-marked bills" (*i.e.,* bait money). After collecting the money, KEAWE left the bank and fled on foot in an unknown direction. F.A. locked the door "for our safety." S.B. later reported an aggregate total of $2,146.99, was missing from her drawer.

11. F.A. described KEAWE as a Polynesian male, in his 60's, tan complexion, with a short grey goatee, 5'10" and 160-170 pounds.

12. HPD conducted area checks to include the area of Pokai Bay, where interviews were also conducted as described below. F.A. had provided HPD a still photograph of the suspect, from the surveillance footage at BOH.

13. HPD interviewed L.A., who was shown a photograph of KEAWE, and immediately responded "that's Rainbow KEAWE." L.A had "just seen" KEAWE walking from Pokai Bay, toward "Middle Park."

14. HPD conducted checks of Middle Park and interviewed K.K., who was shown a photograph of the surveillance footage. K.K. recognized the male in the photograph as "Rainbow," however she did not know his true name or address, but thought he lived near a bridge at "Sewers" Beach Park.

15. C.K. was interviewed and shown a photograph of surveillance footage. C.K. stated the male was known to her as "Uncle Rainbow." C.K. provided his true name as Ellington KEAWE, and stated he was her "hanai" Uncle. C.K. had last seen KEAWE two days ago, and

mentioned his facial features and goatee were the same as when she last saw him. C.K. stated KEAWE had a daughter, A. LNU, and provided her address.

16. HPD went to the address given and asked if "A. LNU," lived there. The woman who answered the door stated she was the mother of "A. LNU" and provided her own name as M.N. M.N. was shown the photograph of the male in the BOH surveillance footage and M.N. immediately stated "that's Ellington KEAWE, my ex-husband." M.N. stated she had seen KEAWE approximately 1700 hours, wearing the same jacket with hood, as seen in the photograph.

17. On May 14, 2019, HPD Detectives conducted a "sequential photo lineup" with six photographs, housed separately in manila folder(s), with the S.B. S.B. positively identified the photograph of ELLINGTON KEAWE, as the male who robbed the bank on May 10, 2019.

18. On May 14, 2019, KEAWE, was arrested by HPD for bank robbery. At the time of arrest, KEAWE, appeared to be wearing the same black, red, and white colored jacket, and carrying a black backpack, similar to that seen in the BOH surveillance footage.

19. The backpack is consistent with the backpack seen worn by KEAWE on the date of the bank robbery as depicted by the surveillance video. In contrast to the backpack seized from KEAWE, however, the backpack seen in the surveillance video, displayed what appeared to be a white and green logo of unknown type or brand, attached to the lower, outer portion of the backpack.

20. On May 15, 2019, HPD Detectives conducted a "sequential photo lineup" with six photographs, housed separately in manila folder(s), with F.A. F.A. picked out a photograph of a male – who was not KEAWE – as the male who robbed the bank on May 10, 2019.

21. The BOH, located at 86-120 Farrington Highway Waianae, HI 96792, was, at the time of the described bank robbery, insured by the Federal Deposit Insurance Corporation (FDIC).

22. The backpack was turned over to the Federal Bureau of Investigation (FBI), on May 15, 2019, by HPD, and is being maintained at the FBI Honolulu Field Office.

23. On May 17, 2019, a federal search warrant was issued in the United States District Court for the District of Hawaii, and signed by United States Magistrate Judge Rom Trader.

24. On May 20, 2019, the aforementioned search warrant was executed on a black in color, "Under Armor" backpack (backpack), seized from KEAWE by HPD, on the date of his arrest. A search of the backpack revealed a silver in color iPhone, housed in a pocket within the backpack. Cell phones are known to house information such as who they belong to as well as location data.

25. KEAWE, is known to be homeless, and it is known, through my training and experience, that those without a house, tend to carry all of their belongings with them everywhere they go, specifically, those items of value.

26. During the course of the bank robbery, the subject was not observed using a cellular device. However, in my training and experience, I know the majority of the population in the United States, is normally in possession of their cellular phone at all times. In fact, in 2018, the Cellular Telephone Industry Association (CTIA), a trade association representing the wireless industry, estimated that 89% of the United States population "always have their cell phones within arm's reach." Therefore, it is reasonable to believe that KEAWE was in possession of the aforementioned cellular telephone at the time of the robbery.

27. In my training and experience, I am also aware that a cellular telephone, such as the Subject Device, is constantly collecting data and communicating with the parent network even when the user is not actively engaged in a voice call or text message conversation. For instance, various applications downloaded on a cellular phone routine operate in the background of the device and can collect information regarding the device's whereabouts, including Global Positioning System (GPS) measurements. This information can assist law enforcement in determining KEAWE's location at the time of the bank robbery.

TECHNICAL TERMS

28. Based on my training and experience, I use the following technical terms to convey the following meanings:

a) Wireless telephone: A wireless telephone (or mobile telephone, or cellular telephone) is a handheld wireless device used for voice and data communication through radio signals. These telephones send signals through networks of transmitter/receivers, enabling communication with other wireless telephones or traditional "land line" telephones. A wireless telephone usually contains a "call log," which records the telephone number, date, and time of calls made to and from the phone. In addition to enabling voice communications, wireless telephones offer a broad range of capabilities. These capabilities include: storing names and phone numbers in electronic "address books;" sending, receiving, and storing text messages and e-mail; taking, sending, receiving, and storing still photographs and moving video; storing and playing back audio files; storing dates, appointments, and other information on personal calendars; and accessing and downloading information from the Internet. Wireless telephones may also

include global positioning system ("GPS") technology for determining the location of the device.

b) GPS: A GPS navigation device uses the Global Positioning System to display its current location. It often contains records the locations where it has been. Some GPS navigation devices can give a user driving or walking directions to another location. These devices can contain records of the addresses or locations involved in such navigation. The Global Positioning System (generally abbreviated "GPS") consists of 24 NAVSTAR satellites orbiting the Earth. Each satellite contains an extremely accurate clock. Each satellite repeatedly transmits by radio a mathematical representation of the current time, combined with a special sequence of numbers. These signals are sent by radio, using specifications that are publicly available. A GPS antenna on Earth can receive those signals. When a GPS antenna receives signals from at least four satellites, a computer connected to that antenna can mathematically calculate the antenna's latitude, longitude, and sometimes altitude with a high level of precision.

c) PDA: A personal digital assistant, or PDA, is a handheld electronic device used for storing data (such as names, addresses, appointments or notes) and utilizing computer programs. Some PDAs also function as wireless communication devices and are used to access the Internet and send and receive e-mail. PDAs usually include a memory card or other removable storage media for storing data and a keyboard and/or touch screen for entering data. Removable storage media include various types of flash memory cards or miniature hard drives. This removable storage media can store any digital data. Most PDAs run computer

software, giving them many of the same capabilities as personal computers. For example, PDA users can work with word-processing documents, spreadsheets, and presentations. PDAs may also include global positioning system ("GPS") technology for determining the location of the device.

d) IP Address: An Internet Protocol address (or simply "IP address") is a unique numeric address used by computers on the Internet. An IP address is a series of four numbers, each in a range of 0-255, separated by periods (e.g., 121.56.97.178). Every computer attached to the Internet must be assigned an IP address so that Internet traffic sent from and direct to that computer may be directed properly from its source to its destination. Most Internet service providers control a range of IP addresses. Some computers have static – that is, long-term -IP addresses, while other computers have dynamic-that is, frequently changed-IP addresses.

e) Internet: The Internet is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

29. Based on my training, experience, and research, and consultation with digital forensic law enforcement agents, I know that the Subject Device has capabilities that allow it to serve as a wireless telephone, a digital camera, a portable media player, GPS navigation device, and PDA. In my training and experience, examining data stored on devices of this type can uncover, among other things, evidence that reveals or suggests who possessed or used the device,

the location of that user or users during specific timeframes, and media that has been created, transmitted, or stored by that user or users.

ELECTRONIC STORAGE AND FORENSIC ANALYSIS

30. Based on my knowledge, training, and experience, and conferral with other law enforcement agents who specialize in the examination of forensic evidence, I know that electronic devices can store information, including information relating to text messages and social media applications as well as metadata collected at the time photographs were taken with the device, for long periods of time. Similarly, things that have been viewed via the Internet are typically stored for some period of time on the device. This information can sometimes be recovered with forensic tools.

31. *Forensic evidence.* As further described in Attachment B, this application seeks permission to locate not only electronically stored information that might serve as direct evidence of the crimes described on the warrant, but also forensic evidence that establishes how the Subject Device was used, the purpose of its use, who used it, and when. There is probable cause to believe that this forensic electronic evidence might be on the Subject Device because:

a) Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file).

b) Forensic evidence on a device can also indicate who has used or controlled the device. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence.

c) A person with appropriate familiarity with how an electronic device works may, after examining this forensic evidence in its proper context, be able to draw

conclusions about how electronic devices were used, the purpose of their use, who used them, and when.

d) The process of identifying the exact electronically stored information on a storage medium that is necessary to draw an accurate conclusion is a dynamic process. Electronic evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

e) Further, in finding evidence of how a device was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium.

f) I know that when an individual uses an electronic device in the commission of an offense on the internet, the individual's electronic device will generally serve both as an instrumentality for committing the crime, and also as a storage medium for evidence of the crime. The electronic device is an instrumentality of the crime because it is used as a means of committing the criminal offense. The electronic device is also likely to be a storage medium for evidence of crime. From my training and experience, I believe that an electronic device used to commit a crime of this type may contain: data that is evidence of how the electronic device was used; data that was sent or received; and other records that indicate the nature of the offense.

32. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit the examination of the device consistent with the warrant. The examination may require authorities to employ techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of the device to human inspection in order to determine whether it is evidence described by the warrant.

CONCLUSION OF THE AFFIANT

33. Therefore, based on my training and experience and the aforementioned facts, I believe probable cause exists for a search warrant authorizing the search of the silver "Apple" iPhone, further described in Attachment A, to seek the evidentiary items described in Attachment B.

Respectfully submitted,

Danielle DeSanctis
Special Agent
Federal Bureau of Investigation

Subscribed and sworn to before me on June 12, 2019

HON. ROM TRADER
United States Magistrate Judge

ATTACHMENT A

Property to Be Searched

The property to be searched is as follows:

1. One (1) silver in color "Apple" iPhone, recovered from the backpack and currently located at the Federal Bureau of Investigation Honolulu Field Office, located at 91-1300 Enterprise Street Kapolei, HI, 96707.

This warrant authorizes the forensic examination of the Device for the purpose of identifying the electronically stored information described in Attachment B.

ATTACHMENT B

Description of the Items to be Seized

1. All records on the subject device described in attachment A, that relate to violation of U.S.C. § 2113(a) and involve Ellington KEAWE, aka "Rainbow KEAWE," as described below:

a. Any and all text messages sent or received, records of communications on any and all social media applications, and all photos sent or received via text messages or social media between May 1, 2019 and May 15, 2019 that tends to show the planning, execution, and/or after actions of the offense in question;

b. Any information regarding Ellington KEAWE, aka "Rainbow KEAWE's" schedule or travel between May 1, 2019 and May 15, 2019;

c. Any and all location information and records, including but not limited to geolocation data, application data, cookies, metadata, and GPS data, and any and all records regarding Ellington KEAWE, aka "Rainbow KEAWE's," physical location from May 1, 2019 – May 15, 2019.

2. Evidence or user attribution showing who used or owned the Subject Device at the time the things described in this warrant were created, edited, or deleted, such as logs, phonebooks, saved usernames and passwords, documents, and browsing history;

This warrant authorizes a review of electronic storage media and electronically stored information seized or copied pursuant to this warrant in order to locate evidence, fruits, and instrumentalities described in this warrant. The review of this electronic data may be conducted by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, and

technical experts. Pursuant to this warrant, the FBI may deliver a complete copy of the seized or copied electronic data to the custody and control of attorneys for the government and their support staff for their independent review.